BUNDESREPUBLIK DEUTSCHLAND

PCT/EP99/07052

EP99/07052

EJU

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern"

am 9. Oktober 1998 beim Deutschen Patent- und Markenamt eingereicht.

Das angeheftete Stück ist eine richtige und genaue Wiedergabe der ursprünglichen Unterlage dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 9/30 der Internationalen Patentklassifikation erhalten.

München, den 12. Oktober 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Aktenzeichen: 198 47 944.1

Brand

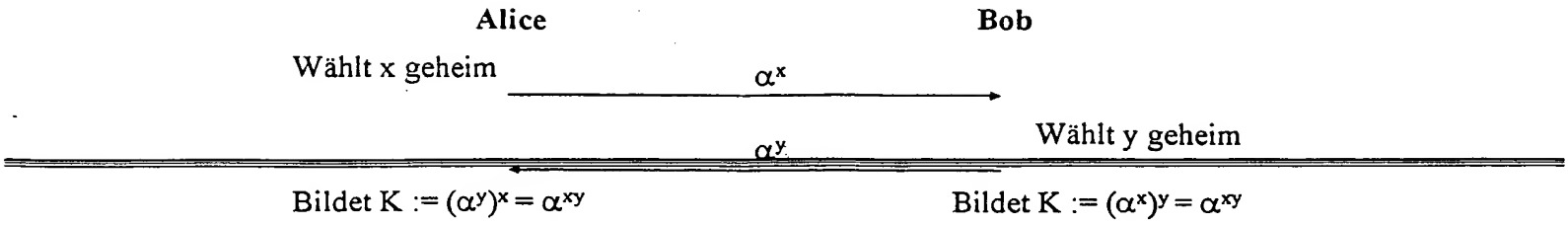
Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern

Beschreibung:

Die Erfindung betrifft ein Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern gemäß dem Oberbegriff des unabhängigen Anspruchs. Verschlüsselungsverfahren in vielfältiger Art gehören zum Stand der Technik und haben zunehmend kommerzielle Bedeutung. Sie werden dazu eingesetzt, Nachrichten über allgemein zugängliche Übertragungsmedien zu übertragen, wobei aber nur die Besitzer eines Krypto-Schlüssels diese Nachrichten im Klartext lesen können.

Ein bekanntes Verfahren zur Etablierung eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist z. B. das Verfahren von W. Diffie und W. Hellmann (siehe DH-Verfahren W. Diffie und M. Hellmann, siehe New Directions in Cryptography, IEEE Transaction on Information Theory, IT-22(6):644-654, November 1976)

Grundlage des DH-Schlüsselaustauschs [DH76] ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren mit x bzw. y einen gemeinsamen Schlüssel $K:=\alpha^{xy}$ berechnen. Ein Angreifer, der nur α^x und α^y sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z.B. von α^x zur Basis α modulo p zu berechnen, und dann α^y damit zu potenzieren.)



Beispiel für Diffie-Hellman-Schlüsselaustausch

Das Problem beim DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob kommuniziert, oder mit einem Betrüger. In IPSec wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z.B. mit endlichen Körpern GF(2^n) oder Elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern.
Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.
Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). Einen Überblick über den Stand der Technik bietet M. Steiner, G.Tsudik, M. Waidner, in Diffie-Hellmann Key Distribution Extended to Group Communication, Proc. 3rd ACM Conference on Computer and Communicatios Security, März 1996, Neu Delhi, Indien.

Eine Erweiterung des DH-Verfahrens auf Teilnehmer A, B und C wird z.B. durch nachfolgende Tabelle beschrieben (Berechnungen jeweils mod p):

	A → B	B → C	C → A
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der Teilnehmer den geheimen Schlüssel $g^{abc} \bmod p$ berechnen.

Bei allen diesen Erweiterungen tritt mindestens eines der folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z.B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl.

Diese Verfahren sind in der Regel schwer zu implementieren und sehr rechenaufwendig.

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000Bit gesendet werden müssen.

Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptographisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren zur Erzeugung eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von mindestens drei Teilnehmern soll den gleichen Sicherheitsstandard wie das DH-Verfahren aufweisen. Das Verfahren soll dabei jedoch einfach zu implementieren sein und einen minimalen Rechenaufwand benötigen. Das

Verfahren soll so ausgebildet sein, daß die geheimen Schlüssel der Teilnehmer der Zentrale dabei nicht bekannt gemacht werden müssen.

Das erfindungsgemäße Verfahren, das dieser Aufgabenstellung gerecht wird, basiert auf den gleichen mathematischen Strukturen, wie das DH-Verfahren und weist daher vergleichbare Sicherheitsmerkmale auf. Im Vergleich zu den bisher vorgeschlagenen Gruppen-DH-Verfahren ist es wesentlich effizienter im Hinblick auf Rechenaufwand und Kommunikationsbedarf.

Nachfolgend wird das Wirkprinzip des erfindungsgemäßen Verfahrens näher erläutert. Die Zentrale wird dabei mit Z bezeichnet, definierte Teilnehmer am Verfahren mit T1-Tn und jeder einzelne nicht konkret benannte Teilnehmer mit Ti. Die öffentlich bekannten Komponenten des Verfahrens sind eine öffentlich bekannte mathematische Gruppe G, vorzugsweise die multiplikative Gruppe aller ganzen Zahlen modulo einer großen Primzahl p, und ein Element g der Gruppe G, vorzugsweise eine Zahl $0<g<p$ mit großer multiplikativer Ordnung. Für die Gruppe G können jedoch auch andere geeignete mathematische Strukturen verwendet werden, z.B. die multiplikative Gruppe eines endlichen Körpers, oder die Gruppe der Punkte einer elliptischen Kurve.

Das Verfahren verläuft in drei Arbeitsschritten.

Im ersten Arbeitsschritt wird von jedem Teilnehmer Ti eine Nachricht der Form $(Ti, g^i \bmod p)$ an die Zentrale gesendet, wobei i eine mittels eines Zufallsgenerators gewählte zufällige Zahl des Teilnehmers Ti ist.

Im zweiten Arbeitsschritt wird in der Zentrale Z

- eine zufällige Zahl z generiert und für jeden Teilnehmer Ti die Zahl $(g^i)^z \bmod p$ berechnet.
- Bei n Teilnehmern werden in der Zentrale Z dann aus diesen n Zahlen n shares mit Hilfe eines an sich bekannten (n, 2n-1) Threshold Verfahrens abgeleitet.
- In der Zentrale Z werden n-1 weitere shares s^1-s^{n-1} ausgewählt und zusammen mit der Zahl $g^z \bmod p$ an alle Teilnehmer T1-Tn gesendet.

Im dritten Arbeitsschritt wird bei jedem Teilnehmer Ti der gemeinsamen Schlüssel k berechnet, wobei

- $(g^z)^i \bmod p = (g^i)^z \bmod p$ berechnet wird,
- daraus ein share des Threshold Verfahrens abgeleitet wird und
- mit diesem share und $s^1,...s^{n-1}$ als Geheimnis der gemeinsame Schlüssel k ermittelt wird.

Nachfolgend wird das erfindungsgemäße Verfahren anhand eines konkreten Beispiels für drei Teilnehmer A, B, und C sowie einer Zentrale Z näher erläutert. Die Anzahl der Teilnehmer ist jedoch auf beliebig viele Teilnehmer erweiterbar.
Bei diesem Beispiel beträgt die Länge der Zahl p 1024 Bit; g hat eine multiplikative Ordnung von mindestens 2^{160}.
Das erfindungsgemäße Verfahren läuft nach folgenden Verfahrensschritten ab:

1. Teilnehmer A, B und C senden $g^a \bmod p$, $g^b \bmod p$ und $g^c \bmod p$ an die Zentrale Z.
2. In der Zentrale Z wird $g^{az} \bmod p$, $g^{bz} \bmod p$ und $g^{cz} \bmod p$ berechnet, wobei jeweils die 128 Least Significant Bits davon als shares s_A, s_B bzw. s_C verwendet werden. In der Zentrale Z wird mittels des (n,2,-1)-Threshold-Verfahrens ein Polynom P(x) über einem endlichen Körper $GF(2^{128})$ vom Grad 2 berechnet, das durch die Punkte $(1,s_A)$, $(2,s_B)$ und $(3,s_C)$ geht und durch diese eindeutig festgelegt ist. Der gemeinsame Schlüssel k ist der Schnittpunkt dieses Polynoms mit der y-Achse, d. h. k; =P(0). Die Zentrale Z sendet nun $g^z \bmod p$, s_1;=P(4) und s_2;=P(5) an die Teilnehmer A, B und C.
3. Beim Teilnehmer A wird $(g^z)^a \bmod p$ berechnet. Im Ergebnis erhält der Teilnehmer A mit den 128 Least Significant Bits dieses Wertes den share s_A, der zusammen mit den shares s_1 und s_2 ausreicht, das Polynom P´(x) und damit auch den Schlüssel k zu bestimmen. Bei den Teilnehmern B und C wird analog verfahren.

Das oben beschriebene Verfahren kommt mit der minimalen Anzahl von zwei Runden zwischen den Teilnehmern T1-Tn und Zentrale Z aus. In der zweiten Runde kann der Aufwand für die von der Zentrale an die n Teilnehmer zu übertragenden Zeichenfolgen

im Gegensatz zu der Lösung von Burmester und Desmedt auf eine Länge von jeweils 128 Bit pro Teilnehmer reduziert werden.

Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern

(1) Patentanspruch:

1. Verfahren zum Etablieren eines gemeinsamen Schlüssels k zwischen einer Zentrale Z und einer Gruppe von Teilnehmern T1-Tn mit einer öffentlich bekannten mathematischen Gruppe G und einem Element $g \in G$ von großer Ordnung in der Gruppe G, so daß für die Gruppe G und das Element g die Berechnung des diskreten Logarithmus praktisch unmöglich ist,

dadurch gekennzeichnet, daß

a) von jedem Teilnehmer (Ti) eine Zufallszahl (i) generiert und aus dem bekannten Element $g \in G$ und der jeweiligen Zufallszahl (i) von jedem Teilnehmer (Ti) der Wert (g^i) berechnet und zur Zentrale (Z) gesendet wird, daß

b) in der Zentrale (Z) eine Zufallszahl (z) generiert wird, daß aus der Zufallszahl (z) und den empfangenen Werten(g^i) die Werte $(g^i)^z$ in G berechnet werden, daß aus diesen Werten n shares $(s_1,...,s_n)$ eines Threshold-Verfahrens abgeleitet werden , und daß aus den shares $(s_1,...,s_n)$ ein (n,2,-1)-Threshold-Verfahren konstruiert wird, wobei das durch dieses Verfahren implizid gegebene Geheimnis der zu etablierende Schlüssel (k) ist, daß in der Zentrale (Z) n-1 weitere, von den shares $(s_1,...,s_n)$ verschiedene shares $(s_{n+1},...s_{2n-1})$ zusammen mit dem Wert g^z in G berechnet und an die Teilnehmer (T1-Tn) übertragen werden, und daß

c) bei jedem Teilnehmer (Ti) der zu etablierende Schlüssel (k) dadurch rekonstruiert wird, daß aus dem von der Zentrale (Z) übertragenen Wert (g^z) und der Zufallszahl (i) des jeweiligen Teilnehmers (Ti) der Wert für $(g^z)^i$ in G berechnet wird, daß aus dem resultierenden Wert mittels eines Threshold Verfahrens der share (s_i) abgeleitet wird und daß mit dem share (s_i) und den von der Zentrale (Z) übertragenen shares $(s_{n+1},...s_{2n-1})$ mit Hilfe des (n,2,-1)-Threshold-Verfahrens der Schlüssel (k) rekonstruiert wird.

1. Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern

2. Zusammenfassung:

2.1. Das vorliegende Verfahren zur Erzeugung eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von mindestens drei Teilnehmern soll den gleichen Sicherheitsstandard wie das DH-Verfahren aufweisen.

2.2. Das Verfahren basiert auf einer öffentlich bekannten mathematischen Zahlengruppe (G) und einem Element der Gruppe $g \in G$ großer Ordnung. Jeder der n Teilnehmer erzeugt eine Zufallszahl (i), berechnet den Wert von g^i in G und sendet diesen Wert an die Zentrale (Z). In der Zentrale (Z) wird ebenfalls eine Zufallszahl (z) generiert und die Werte $(g^i)^z$ in G berechnet. Aus diesen Werten werden die shares anhand eines Threshold-Verfahrens abgeleitet und aus ihnen ein (n,2n-1)-Threshold Verfahren konstruiert. Durch die Zentrale (Z) werden die erzeugten shares zusammen mit dem Werten $(g^i)^z$ an die n Teilnehmer übertragen, die über das (n,2n-1)-Threshold Verfahren den Schlüssel (k) rekonstruieren können.

2.3. Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von mehreren, mindestens jedoch drei Teilnehmern einsetzen.